Teneo®

A Conversation with David Colombo:
From Tesla Hacker to Cyber Risk Advisor

May 2024

David Colombo, the 19-year-old who hacked Tesla cars in 2022 now advises global governments and corporate executives on cyber risk, demonstrating that curiosity can be a powerful source for good.

In March of this year, the *Wall Street Journal* reported on the incredible story of a global band of teenage cyber criminals who hacked casino conglomerate MGM in one of the biggest and most well-known cyber-attacks of 2023. Intrigued by the motivations and mindset of the attackers behind the criminal gang, Teneo Risk sat down with ethical hacker David Colombo, himself a teenager when he became famous for “breaking into” over 25 Teslas around the world from his living room in Germany. David shared details of how he found and reported the security flaws to Tesla, but also discussed the seriousness of today’s cyber threat actors; what he sees as the biggest cybersecurity challenges for organizations today; and how he counsels executives on the risk.

Teneo Risk: ***David, tell us a little bit about yourself, your background, where you're from, how you got into computers and ethical hacking?***

David Colombo: I'm from rural Bavaria, Germany – a town with about 200 people and frankly, cybersecurity isn't really a topic. But I'm just a curious person, if you want to summarize me in one word. I have always asked myself how things work. I got my first laptop for my 10th birthday and thought it was so cool because I was able to connect to the Internet and run different programs. I started wondering how this device could access, manage and process so much at the same time but couldn't find anyone who could really tell me how it all works. Then I discovered that I can Google and research everything myself which really opened up the world of coding to me as well, prompting me to build my first website.

A few years later, when I got into cybersecurity, I found my first security vulnerability by accident and I could see that cybersecurity was going to be one of the most pressing challenges going forward when we have literally digitized our entire lives from smart homes to autonomous cars. I also started to see in the news that hospitals, airplanes and our water infrastructure were becoming targets and the topic grabbed my attention. Eventually, in my mid-teens, I started my own consultancy because I really wanted to work with organizations and use my knowledge to help them protect themselves.

Teneo Risk: ***Let's talk about the Tesla hack. For the record, you are an ethical hacker. This wasn't for criminal purposes. You discovered a vulnerability and explored it, correct?***

David Colombo: Absolutely. I'm not a car guy, I'm a computer guy and Tesla is essentially a computer on wheels. It has a lot more centralized computing than most automobiles. So, coming back again to the topic of curiosity, I wanted to understand how the cars worked. However, I didn't have a Tesla, nor did I know anyone with a Tesla, but every Tesla connects to the Internet for software and application updates which gave me my starting point to explore Teslas from home. I didn't begin with the intention of finding a vulnerability or hacking into something. I just wanted to understand how the car worked. After some research, I discovered that every Tesla connects to something called the "mothership," which is the main server that all the Teslas connect to and communicate with. Further, I found a specific open-source logging tool called TeslaMate which lets Tesla owners monitor data, including a car's energy consumption, location history and music history among other things. Since this logging tool is open source, I was able to review the code myself. Without getting too technical, this is how I found the security flaw which allowed me to access digital keys used to authenticate cars and users. Having access to those digital keys then allowed me to view information about specific cars through TeslaMate. Next, I thought I may be able to send commands to the cars, but I needed to get in touch with owners in order to test that out.

Teneo Risk: ***How did you find Tesla owners?***

David Colombo: Through TeslaMate I could see names of cars. Many Tesla owners name their cars – sometimes using funny or creative names. Similarly, through Google queries, I found social media posts in which car owners talked about their Teslas by name. When I found a match, I reached out to the owner on Twitter (now X) who at first didn't believe that I had access to his Tesla. The first thing he asked me for was the Vehicle Identification Number (VIN) to prove I was serious, so I went back to the logs, got the VIN and messaged it back to him. He confirmed it was his car and then gave me permission to run some "tests." So, I honked his horn and locked his doors which he acknowledged. This was when I knew that Tesla had a potentially serious issue, because I could literally figure out where the car was. If I had been in the car's vicinity, I could have walked up to the car, turned off the security mode, unlocked the doors, climbed in, started the engine and taken a road trip.

Teneo Risk: ***News stories from 2022 noted that you were able to reach 25 cars this way, correct?***

David Colombo: Yes. I tested it with 25 cars because I wanted to see if this was unique to one car or a broader security issue.

Teneo Risk: ***Did you contact Tesla?***

David Colombo: Definitely. After 25 Teslas I knew this was something that had to be addressed with the company. This is where the ethical part comes in. When you find these "bugs" or security flaws, it's necessary to get in touch with the relevant organizations and report it. I consolidated the technical details into a report which covered those 25 Teslas in 13 countries, including Germany, Belgium, Finland, Denmark, the UK, the U.S. and Canada, and sent it to Tesla. The company later revoked thousands of digital keys associated with their cars. In addition, NIST (National Institute of Standards and Technology) rated the security flaw with a 9.8/10, which is "critical."

Teneo Risk: ***Switching gears (pun intended), the very public and high-profile MGM hack that happened in September 2023 was carried out at the hands of a ransomware gang. In March of this year, the Wall Street Journal reported on the story in great detail and we learned that the criminals behind that attack were actually a group of English-speaking teenagers from around the world. These teenagers are clearly not ethical hackers like you. Was this a unique situation with this teenage criminal gang or could we expect to see more of this?***

David Colombo: For me, it was really fascinating when I first learned about the age of those hackers. They are suspected to be between 18 and 24 years' old, so they are still very young and are conducting cyber-attacks against massive organizations. We can see that the age of cyber criminals has dropped significantly over the past decade mainly because it has become so much easier for young people to get access to hacking tools. It may seem very attractive for a teenager because they can just open their laptop, anonymously hack an organization and then ask for $1,000,000 in ransom in one go. There is this

perceived incentive system for young people when it comes to cybercrime, but recent high-profile arrests of cybercriminals by law enforcement will hopefully be a wake-up call to these individuals.

Unfortunately, I don’t think a lot of young people have opportunities to hack for good and are drawn to the bad side of cyber. I've seen it myself in Germany. If you live in a small town without much access to opportunity or encouragement to “do the right thing,” you may be drawn in a different direction.

Teneo Risk: ***Are you discussing this issue with governments and private sector organizations to make them aware of the need to provide awareness, education and opportunities for young people in cybersecurity? How are organizations and governments thinking about incentivizing young people to get into cybersecurity for the right reasons?***

David Colombo: This speaks to education and schools, where it must start very early on. We need to showcase that there are great opportunities for careers in cybersecurity and that it is needed in every industry and every sector. For example, there are cybersecurity jobs in government, big tech, healthcare, entertainment and sports, therefore, it’s important to showcase that you can go anywhere and leverage cybersecurity skills. In my opinion, we have made a lot of progress there. If we look at bug bounty programs, for example, we now have organizations openly offering programs whereby if a hacker finds vulnerabilities, there is an avenue to report them – and in some instances, receive compensation. That was also the case with Tesla. They have a bug bounty program that allows hackers to find vulnerabilities, but they must be reported. The U.S. has made real advances here, but other regions haven’t progressed bug bounty programs in the same way and we need more companies to adopt these policies to increase cybersecurity.

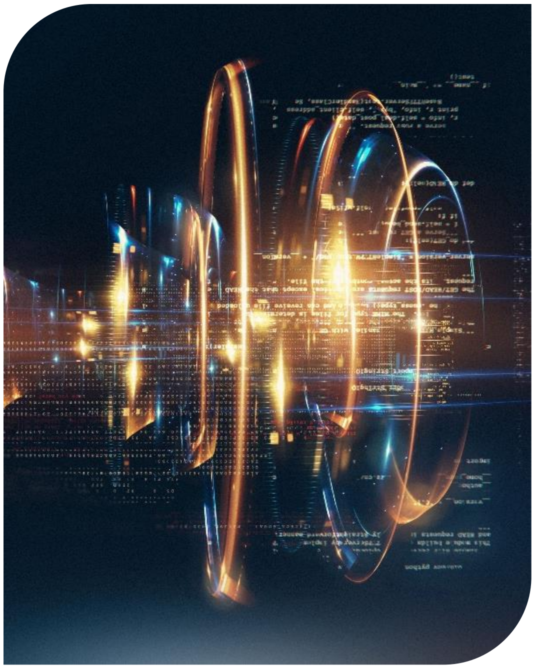
Separately, we need to build programs where we identify young people with critical skills and an interest in cybersecurity and give them opportunities to put their skills to work.

Teneo Risk: ***What are you spending most of your time on at the moment?***

David Colombo: It’s very mixed. I don't think I have the same day twice. On the one hand, I'm doing a lot of consulting. I'm working with organizations to help them better understand cybersecurity from a hacker's perspective, because most organizations only think about cyber risk from a corporate operating perspective. Looking at the problem through the lens of a hacker provides an entirely different viewpoint regarding motivation and intent. Much of the conversation and insights I have access to occurs inside hacker circles. I think sharing that information with a broader audience is of real benefit. Separately, I started coding around the topic of AI and cybersecurity, mainly to learn a bit more about the opportunities that we have, as well as to be able to anticipate the potential dangers facing organizations on the more nefarious side of AI. All in all, I stay pretty busy between consulting, traveling for keynotes at conferences or conducting really technical research in the cybersecurity space.

Teneo Risk: ***What do you worry about in terms of the future of cyber risk? What should organizations and executives be focused on?***

David Colombo: This is a good question. At the end of last year, I was at an event at NVIDIA having this precise discussion with a group of Fortune 500 CISOs. Interestingly, regardless of which industry the CISOs came from, they all commented on concerns over the cloud and cloud migration, because so many organizations are moving to the cloud which has become a major part of their business and technology strategy. We agreed that you cannot run cloud operations the same way that you ran your legacy data centers because being “in the cloud” has created a different set of attack vectors. This expanded attack surface has significantly broadened because so many more of our services are exposed to the Internet. At the same time, there are so many more configurations within cloud infrastructure – if just one checkbox or configuration is incorrect, you could have massive exposure and hackers know this.



The second area that hopefully executives are focused on is software supply chain. We saw yet another story unfold just a few weeks ago when a Microsoft developer disclosed a backdoor in XZ Utils which impacted all Linux servers. Luckily the security vulnerability was spotted in time, but interestingly the only reason the issue was discovered was because one Microsoft engineer noticed a 500-millisecond delay in one of his code executions. If that hadn't happened, hackers would have had a nice backdoor into a massive global collection of servers. While we are making progress in protecting our software supply chain, there are still so many vulnerabilities in the way software is designed and built. Broadly, I think about managing supply chain risk in three pieces, starting with visibility. The software development lifecycle or "SDLC" has become so complex and generally, there is not a lot of visibility into software development processes including how security is built into the SDLC and we need to get better here. The second part for me is protection using security frameworks, security guidelines and policies that we enforce and implement. The last piece is really detection and response. We will all get hacked eventually, whether through a zero-day exploit, which is an exploit that no one yet knows about, or a simple click of an email or targeted phishing attack. So, the more visibility we have, the more adherence to security frameworks and advanced detection and response, the better positioned we are to protect our technology supply chain.

The third area of focus is of course, cybersecurity and AI. We are only at the beginning of identifying the cybersecurity risk associated with the deployment of AI. From the use of ChatGPT to Large Language Models, we need to be able to ensure data quality and secure data usage to prevent potentially dangerous actions or outcomes.

Teneo Risk: ***How do you advise C-suite executives and board directors to approach the topic of cybersecurity, especially if their role is not intended to be in the technical weeds?***

David Colombo: I think that is a fantastic question because there needs to be a translation layer between the really technical topics and the discussion around business risk or financial risk within an organization. That translation enables a conversation around acceptable and unacceptable risk. We need to zoom out of the conversation from a focus on the acute technical problems in cybersecurity to an analysis of how disruption and risk may impact the overall business and business strategy. Approaching cybersecurity risk in terms of business impact will drive the discussion right to the C-suite and board. When executives ask me how to think through cybersecurity, I always push them to work more closely with the CISO and work toward assigning the right business and financial data points to the risks.

One other key point here relates to the issue of cybersecurity expertise at the board level. If we look at the U.S., according to new SEC regulation, every public company now needs to disclose the board's oversight of cybersecurity risk, which I think is a great step in the right direction because the cybersecurity conversation has to take place at the board level. I think this creates an interesting career pathway for CISOs, potentially carving out opportunities for CISOs to progress to board director positions.

***Teneo Risk:* Any final thoughts you would like to leave us with?**

David Colombo: My final comment relates somewhat to the last question and the Tesla story. Since we have all of these physical assets connected to the Internet, the risk now extends to human life. When we consider the potential vulnerability and exposure of hospitals, cars, airplanes, water infrastructure and our power grids, cybersecurity then becomes about protecting human lives as well. We can't have boards and companies not caring about or de-prioritizing the topic. Some companies, by virtue of their business or their sheer size, have to care about espionage or nation-state threat actors. But regardless of your business size or operating model, cybersecurity needs to be at the forefront and cybersecurity awareness needs to be driven from the top down.

For more information, email: Resilience&Intelligence@teneo.com

Authors

Courtney Adante
President, Security Risk Advisory
Courtney.Adante@teneo.com

David Colombo
Keynote Speaker, Advisory Board Member, Startup Founder and Globally Recognized Cyber Security Expert

Teneo
The Global CEO Advisory Firm

Teneo is the global CEO advisory firm.

We partner with our clients globally to do great things for a better future.

Drawing upon our global team and expansive network of senior advisors, we provide advisory services across our five business segments on a stand-alone or fully integrated basis to help our clients solve complex business challenges. Our clients include a significant number of the Fortune 100 and FTSE 100, as well as other corporations, financial institutions and organizations.

Our full range of advisory services includes strategic communications, investor relations, financial transactions and restructuring, management consulting, physical and cyber risk, organizational design, board and executive search, geopolitics and government affairs, corporate governance, ESG and DE&I.

The firm has more than 1,600 employees located in 40+ offices around the world.

teneo.com